從原則邁向 IT 系統實踐之路（上）

落實隱私應始於設計

個資保護觀念愈來愈重要，個資保護結合設計思維已成顯學，然而無法掌握其原則與精神卻是難以施展，資料安全落實在系統開發生命週期，如何善盡隱私保護之責已成重要課題。

文／林逸塵（國立政治大學資訊管理博士）

現今人工智慧及資通技術快速發展，資料驅動（data-driven）成為創造知識及提供服務的催化劑，過程中要發掘「資料價值」與「資料治理」同等重要。例如：資料可以用於訓練人工智慧模型、個人化管理及精準行銷等用途，當蒐集數據極大化時，將增加隱私風險及系統開發的複雜度，對資訊隱私將造成極大衝擊，企業確保數據安全已視為責任，然而在促進個人資料的合理運用更加重要。

因此，從個人資料加值的角度，要達成破壞式創新（disruptive innovation）的前提，應要先透過資料保護影響評估（Data Protection Impact Assessment；DPIA），由資料控管者所執行的紀錄程序，敘述、評估及管理 IT 專案的隱私或資料保護風險，以檢驗基本人權是否獲得充份保障。

此外，保障個人資料安全可透過「設計思維」達成，例如：**隱私始於設計（Privacy by Design, PbD）**是跨學門領域的資訊管理方法，這種思維所表述的哲學及方法論，可以應用在特定的 IT 技術、業務運營、物理架構及網路基礎設施等，並在 IT 系統開發中貫穿整個資料流與生命週期，實踐在整個資訊生態系及治理模型。

資料生命週期與隱私安全風險

所謂資料生命週期的各階段，包括資料蒐集、保留、記錄、產生、轉換、使用、揭露、共享、傳輸、處置、銷毀等操作。為嚴格遵循必要性及合乎比例之個人資料處理，在資料蒐集、處理及利用當下，應優先考慮資料安全的措施。例如：依照資料機密級別透過指定網路或資訊系統存取，防止資安事件造成違法或惡意行為危害；對於儲存或傳輸之個人資料，確保其資料可用性、完整性及機密性，避免網路或系統造成個資的危害；透過**電腦緊急應變小組（Computer Emergency Response Team；CERT）**、**電腦資訊安全事件應變小組（Computer Security Incident Response Team；CSIRT）**、網路及系統服務供應商所提供安全服務；防止非經授權之網路存取及阻擋惡意程式之散播、防止阻斷服務攻擊（DDoS）造成電腦系統損害，也就是資料控管者提供符合使用者期待的資料安全防護。

當個人資料透過 IT 系統的大規模蒐集，當事人之權利及自由將面臨多重風險，例如，資料在生命週期中，因人為不當的操作造成身體、財物或聲譽損害，以下舉例可能的隱私安全風險情境：

- 當處理造成歧視、身分盜用（或詐欺）、金融損失、名譽損害、受秘密保護之個人資料外洩；
- 假名化資料未經授權的還原，造成當事人的權利侵害、失去個人資料控制權；
- 當資料處理涉及揭露種族或人種、政治意見、宗

教或哲學信仰、基因、健康、性生活或前科及犯罪資料時；

- 當個人特徵受到評價，個人剖繪（profiling）用於分析工作表現、經濟狀況、健康、個人偏好或興趣、可信度，預測行為、地點或動向等個人隱私時；
- 當處理兒童被害人之個人資料或牽涉大量個人資料時，以上皆有影響資料主體重大利益的風險。見（**圖 1**）

為確保個人資料保護，組織須採取適當之科技上、程序上措施，資料控管者應採用資料保護設計與預設（by design & default）的規則。

例如：資料最小化（minimising）及假名化（pseudonymising），提升透明度、使資料控管者提升安全性功能、保有資料與目的相關性。因此，在開發設計及選用處理個人資料之 IT 系統、應用程式、服務與產品時，確保資料保護納入預設之考量，以利資料控管者及受託者得以善盡義務。

在公開招標過程中，PbD 應在採購規格中列為需求，使系統開發得以遵循。此外，因為技術、執行成本、業務性質、範圍及開發目的不同，對當事人行使權利的方式不同，應採取可及時回復個人資料可用性及可接近性，透過定期評估、測試、衡量以確保安全措施之有效性。

全球隱私標準的關鍵要項

我們先從 1973 年**公平資訊實務原則（Fair Information Practice Principles；FIPPs）**來理解，FIPPs 的概念是出自於美國聯邦政府衛生、教育和福利諮詢委員會的「紀錄、電腦和公民權利」（Records, Computers and the Rights of Citizens）報告，其已被納入世界各地許多組織的政策中，包括透明化、當事人參與、監管、目的說明及使用限制、資料最小化、資料品質及完整性、存取及修正、資料安全、問責性等隱私推定預設原則。見（**圖2**）

全球隱私標準（Global Privacy Standard；GPS）是一套普遍隱私原則，成為現今公平資訊實踐中最佳的原則，GPS 是在 2006 年 11 月 3 日第 28 屆國際數據保護與隱私專員會議上被提出，之後獲得全球廣泛接受。該標準是基於國際數據保護團體的群眾知識和實踐智慧，採取單一及易於理解

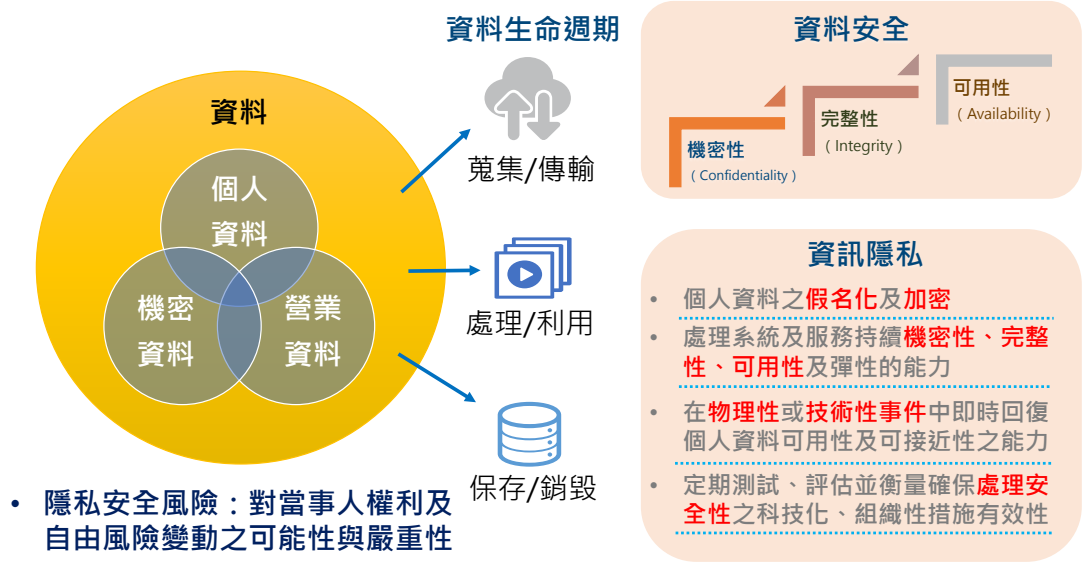

圖1 資料生命週期與隱私安全風險示意

圖2 美國聯邦政府公平資訊實務原則

的標準格式呈現。

GPS 提示 IT 系統開發者及使用者，在管理上或處理資訊新技術和系統功能，GPS 在開發 ICT 技術標準、規範、協議及相關的合規評估實踐時特別有意義，以下說明 GPS 的關鍵要項：

1. **同意（Consent）**：個人必須自由且明確地同意蒐集、使用或揭露個人資料，除非法律另有其他合法規定要件。資料的敏感性越高，所需的同意品質要求會越高，也更需要清晰和具體，並且同意是可以在日後經當事人撤回。

2. **問責（Accountability）**：蒐集個人資料需要承擔保護的責任，包含所有與隱私相關的政策和程序，其執行責任應適當記錄及傳達，並指派給組織內的特定資料處理人員。當個人資料轉移給第三方時，組織應透過契約或適當方式達成同等的隱私保護程度。

3. **目的（Purposes）**：組織應明確說明蒐集、使用、保留及披露個人資料的目的性，並在蒐集個人資料前（或處理當下）將目的告知資料主體，且特定目的應要符合明確性、有限制及與該情境相關的要件。

4. **蒐集限制（Collection Limitation）**：蒐集個人資料必須公平合法，並限於為特定目的所必需的範圍內。資料最小化（Data Minimization）是指蒐集個人資料應保持嚴格的最低限度。作業程序、資訊技術及系統設計應採取非可識別的互動(交易)作為預設選項，隨時保持最小化個人資料的可識別性、可觀察性及可連結性。

5. **使用、保留及揭露限制（Use, Retention, and Disclosure Limitation）**：組織應限制對個人資料的使用、保留及揭露，僅限於向個人所識別的相關目的，除非法律上另有要求，個人資料應僅在滿足特定目的所需的期間內進行保留，最終進行安全銷毀。

6. **準確（Accuracy）**：組織應確保個人資料的正確性、完整性及最新性，以滿足特定目的對於資料品質的需要。

7. **安全（Security）**：組織必須對個人資料在生命週期內的安全負責，並遵循廣泛認可的標準組織制定的國際標準（例如：ISO 27701）透過合理的保障措施，所採取措施應依據資料的敏感性而適當對應（包括物理、技術和管理手段）。

8. **開放（Openness）**：開放性和透明度是問責的關鍵，與個人資料管理相關的政策和實踐的資訊應該隨時向個人提供，以利資料主體瞭解隱私政策，及便利當事人主張資訊控制的權利。

9. **存取（Access）**：個人應有權存取自己的個人資料，並獲知其使用和揭露情形，個人有權質疑資訊的準確性和完整性，並可視需要進行修改或向資料控管者提出主張。

10. **合規（Compliance）**：組織必須建立申訴及補救機制，並向公眾傳達相關的訊息，包括如何進行下一階段的救濟。組織應採取必要的監控、評估及驗證其隱私權政策與作業程序的合規情形。

隱私始於設計的七項原則

隱私始於設計是一種系統設計的框架，最早由加拿大安大略省前資訊和隱私專員 Dr. Ann Cavoukian 在 90 年代提出的概念。PbD 的七項原則對於指導 IT 系統發展方向具相關性及重要性，許多資料保護專家已廣泛認可並引用，可以用於制定更細部的系統開發原則、稽核和驗證的標準，隱私保護在預設情況下，必須納入資料、網路、系統等技術採用的考量，而且深化到組織開發系統時的優先事項，在資訊專案目標、流程設計及營運規劃不

可或缺的一部分。見（**圖 3**）。

對照前一節所述的 GPS 關鍵要項，在政府管理資訊系統（特別在個人資料處理）至關重要，其核心原則與組織的隱私管理實踐相關。「隱私始於設計」再進一步將全球認可的隱私標準吸納並且概念化，以下為隱私始於設計的七項原則。此外，隱私始於設計（PbD）擴大了公平資訊普遍原則（FIPP）實踐概念，代表隱私保護領域標準的顯著提升，兩者間有其對照關係。見（**表1**）

‖ 原則1：主動非被動：預防非補救（Proactive not reactive：preventative not remedial）

PbD 是一種主動而非被動措施，要防範於發生侵犯隱私事件前，即因為系統衍生的隱私風險預測及預防措施。PbD 不是提供解決隱私違規事件發生後的補救措施，其目的是識別風險並預防危害的發生，因此 PbD 是在事前而非事後進行的。

‖ 原則2：隱私保護為預設選項（Privacy as the default setting）

當系統開發導入 PbD 時，其系統已將隱私保護成為初始預設規則，隱私設計旨在確保任何 IT 系統或業務實踐流程中，自動保護個人資料以提供最大程度的隱私防護。即使個人不採取任何行動下，其隱私仍然完好無損，隱私在預設情況已經內建在系統的流程、功能或組態。

‖ 原則3：隱私措施內嵌於設計（Privacy embedded into design）

隱私措施採取融入 IT 系統和業務實務設計及架構之中。而非在事後作為附加的元件添加的。隱私保護機制是成為所提供核心功能的重要組成部分，因此隱私是系統不可或缺的一部分，且同時不會削弱系統既有功能。

‖ 原則4：隱私設計全方位賦能（Full functionality：positive-sum, not zero-sum）

PbD追求以「正和雙贏」的方式滿足所有合法利益及目標，而不是以過時的「零和遊戲」(非此即彼)的方式進行非必要的設計權衡。PbD避免了隱私與安全間產生二分法的謬誤，其證明系統在隱私功能的權衡確實是能夠兼得的。

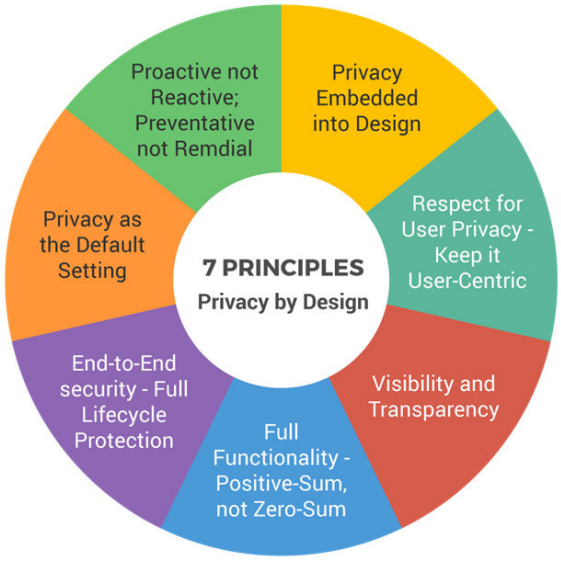

圖3，隱私始於設計的七項基本原則

‖ 原則5：貫穿生命週期安全保護（End-to-end security：full lifecycle protection）

PbD 在收集第一個資訊元素前就已嵌入系統中，並安全地延伸至所涉及個人資料的整個生命週期，自始至終、強而有力對於隱私保護的安全措施，以確保所有資料都及時安全地蒐集、處理、保留及銷毀，確保個人資料的機密性、完整性及可用性。因此，PbD 是確保資料從出生到消滅、貫穿資訊安全的生命週期管理。

‖ 原則6：可見及透通的開放運作（Visibility and transparency：keep it open）

PbD 旨在向所有利益相關者保證，無論涉及各種技術或商業實踐，實際上都會按既定的承諾及目標運作，並可以接受核實的獨立驗證。資料主體明瞭其被蒐集的個人資料及其目的，對於 IT 系統的使用者及提供者而言，所有元件及運作都是可見及透明的，以此建立數位信任基石。

‖ 原則7：尊重隱私以用戶為中心（Respect for user

Privacy by Design Foundational Principle	Fair Information Practice Principle
1. Proactive not Reactive; Preventative not Remedial	
2. Privacy as the Default	● Purpose Specification ● Collection Limitation ● Data Minimization ● Use, Retention and Disclosure Limitation
3. Privacy Embedded into Design	
4. Full Functionality - Positive-Sum, not Zero-Sum	
5. End-to-End Lifecycle Protection	● Security
6. Visibility and Transparency	● Accountability ● Openness ● Compliance
7. Respect for User Privacy	● Consent ● Accuracy ● Access

表1、PbD與FIPPs的原則間對照關係

privacy：keep it user-centric）

PbD 要求系統架構師和營運商透過提供隱私預設值、適當的通知或授權使用者友善選項等措施，將個人的利益放在第一位，目標在數位化互聯網的世界中，確保以用戶為中心的隱私，並將使用者優先的隱私功能設計為核心。

隱私始於設計與資訊系統開發

組織採用「隱私始於設計（PbD）」架構，在最初階段就應對隱私及資料保護問題進行因應。世界各地的主管機關已經體認到這種方法的優點，由歐盟 GDPR 制訂可知，其在處理歐洲公民資料為必要的要求。企業若希望將隱私全面整合至其基礎架構中，資料最小化是僅向客戶收集需要的資料，用於使用者同意的用途，並遵循適當的資料保留政策，或在達成預期目的後刪除資料。

假名化能夠讓個人資料無法直接識別出特定人士，要將個人資料連結到特定某人的唯一方法，是將它與分開儲存及保護的其他資料組合在一起。這表示組織仍在處理個人資料為客戶提供服務時，同時也能保護客戶隱私權，這些原則都可以做為保護資料隱私的措施，並在整個系統設計生命週期中提供決策。

當我們享受數位轉型帶來的便利及效率，同時也必須重視個人操控資訊的自由選擇，資訊自決權（the right of self-determination of personal information）是對於個人資料自主控制的權利，包含決定是否揭露個人資料，以及在何種範圍內、在何時、以何種方式、向何人揭露的決定權。

尤其在數位化的時代，IT 系統在開發時就必須導入隱私始於設計（PbD）的思維，如此才能將系統保有的個人資料的目的與功能連結。

下一期將進一步介紹，透過 PbD 的核心概念，轉換為以「資料保護設計」的系統實踐方式，將隱私始於設計（PbD）與 IT 系統的開發實務作更深入的介紹。

作者林逸塵任職於個人資料保護委員會籌備處隱私科技組組長，具有廿年以上資安及資訊管理相關經歷，專業領域在個人資料安維、資通訊安全、人工智慧、系統設計科學、資訊策略及新興技術應用，並發表多篇相關領域文章及學術期刊。